Remarks/Arguments

Claims 1-20 are pending. Claims 1-7 and 10 stand rejected under 35 U.S.C. 103(a) as being unpatentabe over Schneier (select portions of "Applied Cryptography", 2nd Ed.). Claims 8, 9 and 11 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Arnold (United States Patent No. 5,787,172). Claims 12–20 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier in view of Arnold, and further in view of Force (United States Patent No. 5,533,123).

Applicant respectfully traverses these rejections, and request reconsideration of the pending claims for at least the following reasons.

35 U.S.C. §103(a) sets forth in part:

> [a] patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.

To establish a prima facie case of obviousness, all of the recited claim limitations must be taught or suggested in the prior art. *See, MPEP 2143.03; see also, In re. Royka, 490 F.2d 981, 180 USPQ 580 (CCPA 1974).* Further, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to combine reference teachings. *See, M.P.E.P. 706.02(j).* Further yet, the teaching or suggestion to make the claimed combination must be found in the prior art, and not based on the applicant's own disclosure. *In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).*

Applicant respectfully submits: (1) the cited prior art fails to teach, or suggest, each of the recited limitations of any of the pending claims; and, (2) a proper motivation and reasonable expectation of success for modifying the teachings of Schneier in the manner argued is lacking for at least the following reasons.

1. Claims 1 - 9 - A method for managing access to a device.

The present invention as recited in present claim 1 is directed to:

> A method for managing access to a device, said method comprising:
> (a) sending a first message from a first device to a second device;
> (b) receiving, in said first device, from said second device a digital certificate encrypted using a first private key of said second device;
> (c) receiving, in said first device, from said second device said first message encrypted using a second private key of said second device;
> (d) authenticating said second device in response to said digital certificate and said first encrypted message; and
> (e) establishing a communication channel between said first and said second devices in response to the authentication of said second device.

The claimed method enables a device such as a set-top box to authenticate a second device such as a server or other such device associated with a service provider, before a communications channel is established between the two devices. To accomplish this, the first device sends a message to the second device. The first device receives a digital certificate from the second device. The digital certificate includes a portion that is encrypted via a private key of the second device. The first device further receives from the second device the first message that was originally sent by the first device, but in an encrypted form using a second private key of the second device. The digital certificate and the first encrypted message are then used to authenticate the second device. Upon authentication, a communications channel is established between the first and second devices.

1.1. <u>The Key and Message Transmission Section on Page 51 of Schneier Does Not Teach an Authentication Protocol.</u>

The Office action first argues Schneier teaches a basic authentication protocol in the Key and Message Transmission Section on page 51. *See, 1/19/2005 Office action, par. 12, lines 1 – 5.* Applicant traverses this assertion. While the

present invention is generally directed to "providing conditional access in [a] set-top box so that the box can only connect to selected service providers", the referenced portion of Schneier is instead directed to securely exchanging a message M.

That is, the referenced portion of Schneier does not teach or suggest an authentication scheme at all, but rather teaches a method for securely exchanging a message M without requiring a prior key-exchange protocol. Indeed, as Schneier expressly teaches that Alice encrypts the symmetric key K using Bob's public key, Bob cannot use the method of the referenced portion of Schneier to authenticate Alice, since Bob's public Key is not restricted to Alice and is instead generally ascertainable by others.

Accordingly, Applicant respectfully submits the Key and Message Transmission Section on page 51 of Schneier fails to teach, or even suggest, any authentication protocol or scheme. Further, Applicant traverses any assertion that encrypting using a public key is "effectively equivalent" to encrypting using a private key. In contrast, encrypting using a public key generally enables one to secure content for a particular recipient *(see, e.g., Schneier page 51)* while encrypting using a private key generally allows for the public to access the content *(see, e.g., Schneier, page 54)*.

Consequently, the protocol discussed in the Key and Message Transmission Section on page 51 of Schneier, even taking into account the Examiner's proposed modifications, fails to teach or suggest each of the recited limitations of Claim 1, as the portion of Schneier identified by the Examiner teaches a method for securely exchanging a message M and not an authentication scheme. Further, a proper motivation and reasonable expectation of success for making the proposed modifications is lacking, for at least the following reasons.

1.2. The Cited Portions of Schneier Do Not Teach or Suggest the Claimed Steps (a) and (c) of Present Claim 1.

Claim 1 recites, in part: "(a) sending a first message from a first device to a second device", and "(c) receiving, in said first device, from said second device said first message encrypted using a second private key of said second device."

Accordingly, Claim 1 requires a first device send a message to a second device, and then receive that same message back from the second device in an encrypted form. The Schneier reference fails to teach or suggest these limitations.

The Office action argues Schneier teaches a node A receiving two encrypted messages: the principle message (M) encrypted with a symmetrical key K ($E_k(M)$), and the symmetrical key K encrypted by node A's public key ($E_A(K)$). Node A retrieves key K by decrypting the key message ($D_A(K)$), and then uses the decrypted key K to retrieve message M ($D_k(M)$). Again, Applicant respectfully points out this is not an authentication scheme at all, but rather a method for securely exchanging a principle message (M) without requiring a previous key exchange.

The above notwithstanding, the Office action admits the Key and Message Transmission Section on page 51 of Schneier and digital certificate discussion on pages 576-577 of Schneier fail to teach the Claim 1 steps (a) and (c) – in at least that it admits "this modified authentication scheme does not disclose the step of node A submitting the original principle message to node B." *1/19/2005 Office action, par. 14, lines 1-2.* The Office action attempts to remedy this admitted shortcoming by arguing these steps correspond to simple challenge requests and responses initiated by node A, returned by node B, and verified by node A. *1/19/2005 Office action, par. 14, lines 1-5.* The Office action goes on to argue that Schneier teaches challenge protocols, and that it would have been obvious at the time of invention to use the principle message (M) as a challenge value to authenticate the identity of node B and the timeliness of the message received from node B. *1/19/2005 Office action, par. 14, lines 6-14.*

Applicant traverses this assertion, and submits Schneier actually teaches against such a modification for at least the following reasons.

The purpose of the protocol described in the Key and Message Transmission Section on page 51 of Schneier is to allow for a secure exchange of principle message (M) (through encryption $E_k(M)$) without requiring a prior exchange of key K. *See, Schneier, page 51, lines 2-3 ("Alice and Bob need not complete the key-exchange protocol before exchanging messages").* If nodes A and B intended for message M to be sent in a manner that makes it publicly available, it would not be encrypted with symmetrical key K in the first place. *See, Schneier, page 51, lines 3-*

6 ("In this protocol, Alice sends Bob the message, M, without any previous key exchange protocol: (1) Alice generates a random session key, K, and encrypts M using K $E_K(m)$"). Thus, the referenced protocol expressly teaches message M is secured in a manner that restricts access to the intended recipient, Bob. *See, Schneier, page 51, lines 8-11 ("(3) Alice encrypts K with Bob's public key $E_B(K)$; (4) Alice sends both the encrypted message and encrypted session key to Bob $E_K(M)$, $E_B(K)$").*

Applicant submits these teachings of Schneier must be considered in determining whether or not the proposed modification would have been obvious at the time of invention, as a prior art reference must be considered in its entirety (i.e., as a whole), including portions that would lead away from the invention at issue. *See, Panduit Corp. v. Dennison Manuf. Co., 810 F.2d 1561, 1 USPQ2d 1593 (Fed. Cir. 1987).* The mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. *See, M.P.E.P. §2143.01; see also, In re Mills, 916 F.2d 680, 16 USPQ2d 1430 (Fed. Cir. 1990).* For example, where a proposed modification would render the prior art invention modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *See, In re,. Gordon, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984).*

Applicant submits it would not have been obvious to modify the referenced key and message exchange protocol of Schneier to use the principle message (M) as a challenge value, because such a modification would render the protocol unsuitable for its intended purpose of securely exchanging a principle message (M) without requiring a previous key exchange.

More particularly, the proposed modification of Schneier would send the principle message (M) in a manner that permits for uncontrolled access to message (M), thereby completely eviscerating any need for key (K) or any other portion of the protocol of the Key and Message Transmission Section on page 51 of Schneier. For example, the first four (4) steps on page 54 of Schneier require that Alice encrypt a random string she received from a host with her private key, and return it to the host. This allows the host to look up Alice's public key, decrypt the random string and compare it to the original random string. The Office action essentially proposes

using the principle message (M) in place of the random string. *1/19/2005 Office action, par. 14, lines 11-14.*

However, such a challenge protocol using principle message (M) eliminates any need for the protocol of the Key and Message Transmission Section on page 51 of Schneier, as both parties would already have access to principle message (M). Furthermore, Schneier does not teach that the random string (the challenge value) is protected during transmission from the host to Alice in any manner, and thus contradicts the entire purpose of the protocol of the Key and Message Transmission Section on page 51 of Schneier. Still further, Schneier teaches that Alice's private key is used to encrypt the random string to allow the host (which does not have access to Alice's private key) to decrypt the message using her public key. Because a private key is used to encrypt the principle message (M) – which is expressly required by the first four steps on page 54 of Schneier to enable the host to access the encrypted random string – the protocol of the Key and Message Transmission Section on page 51 of Schneier would necessarily fail. Access to key K and hence the principle message (M) would not be restricted to the intended recipient in the proposed modified scheme, but could be decrypted by any person having the ability to look up public keys.

Thus, the proposed modification would render the secure key and message exchange protocol of page 51 of Schneier unsatisfactory for its intended purpose, as it would fail to secure the principle message (M).

Applicant submits a proper motivation for modifying the protocol of the Key and Message Transmission Section on page 51 of Schneier with the discussion of Yahalom (pages 57-58) is similarly lacking. Again, the purpose of the protocol described in the Key and Message Transmission Section on page 51 of Schneier is to allow for a secure exchange of principle message (M) (through encryption $E_K(M)$) without requiring a prior exchange of key K. However, Yahalom expressly teaches that users share keys ("the key [Bob] shares with Trent ... the key [Trent] shares with Alice"). Accordingly, this proposed modification would also render the protocol of the Key and Message Transmission Section on page 51 of Schneier unsatisfactory for its intended purpose, because it would require a previous key exchange.

For purposes of completeness, Applicant also submits Schneier's teachings on page 38 (Signing Documents and Timestamps) fail to add anything with regard to the admitted shortcomings of the Key and Message Transmission Section on page 51 of Schneier, as it merely sets forth a rationale for including timestamps with signatures (e.g., to stop Bob from cashing a single digital check more than once).

Accordingly, Applicant respectfully requests reconsideration and removal of the rejection of Claim 1 as being unpatentably obvious of Schneier, at least by reason that: (1) Schneier fails to teach, or suggest, (a) sending a first message from a first device to a second device, and (c) receiving, in said first device, from said second device said first message encrypted using a second private key of said second device; and (2) that a proper motivation and expectation of success for the proposed modification to the teachings of the Key and Message Transmission Section on page 51 of Schneier is lacking – at least by reason that the proposed modification would render the protocol unsatisfactory for its intended purpose (i.e., securely exchanging message M).

Applicant also respectfully requests reconsideration and removal of all rejections of Claims 2 – 9, at least by virtue of these Claims' ultimate dependency upon a patentably distinct base Claim 1.

1.3. <u>The Cited Portions of Schneier Do Not Teach or Suggest the Claimed Step (b) of Present Claim 1.</u>

Claim 1 also recites, in part, "(b) receiving, in said first device, from said second device a digital certificate encrypted using a first private key of said second device." Applicant submits Schneier also fails to teach, or suggest, such a limitation. Rather, Schneier expressly teaches the use of a third-party Certificate Authority (CA). *See, e.g., Schneier, pages 575 – 577.*

For non-limiting purposes of explanation only, reference may be drawn to page 6, lines 16-18 of the present specification, wherein it teaches, "it is within the scope of this invention that the role of Certificate Authority may be performed by [service provider] SP 40 in collaboration with the manufacturer of the STB 20."

In contrast, Schneier only teaches certificates generated using a private key of a third-party Certificate Authority (CA). For example, Schneier teaches a trusted

Certificate Authority (CA) issues CA signed certificates. *Schneier, pages 575-576.* Further, Schneier teaches two possibilities for verifying certificates: where Alice and Bob share a third-party CA and Alice simply verifies the CA's signature on Bob's certificate; and, where Alice and Bob use different third-party CA's, and a certificate hierarchy with a common third-party CA is used.

Neither of these scenarios meets step (b) of Claim 1, which recites that the certificate received by the first device, from the second device (with whom a communications channel is established as recited in step (e)), is encrypted using a private key of the second device, and not a third party CA. That is, Claim 1 requires that the certificate be encrypted with a private key of the second device itself – a condition contrary to the teachings of Schneier, which uses one or more third party CA's to sign certificates. For purposes of completeness, Applicant submits Schneier provides no motivation for modifying its teachings with regard to Certificates and issuing CA's to meet the limitations of Claim 1.

Accordingly, Applicant respectfully requests reconsideration and removal of the rejection of Claim 1 as being unpatentably obvious of Schneier, at least by virtue that Schneier also fails to teach, or suggest, (b) receiving, in said first device, from said second device a digital certificate encrypted using a first private key of said second device. Applicant again respectfully requests reconsideration and removal of all rejections of Claims 2 – 9, at least by virtue of these Claims' ultimate dependency upon a patentably distinct base Claim 1.

1.4. The Cited Portions of Schneier Do Not Teach or Suggest the Claimed Use of First and Second Private Keys Recited In Steps (b) and (c) of Claim 1.

Claim 1 recites, in part, "(b) receiving, in said first device, from said second device a digital certificate encrypted using a first private key of said second device", and "(c) receiving, in said first device, from said second device said first message encrypted using a second private key of said second device". Thus, Claim 1 recites using first and second private keys of the second device.

Applicant respectfully submits Schneier fails to teach, or suggest, using multiple private keys of a single device. Rather, Schneier merely teaches public-

private key cryptography pairs, such as those proposed by Whitfield Diffie and Martin Hellman (Diffie-Hellman). *See, e.g., Schneier, pages 31-34.*

Accordingly, Applicant respectfully requests reconsideration and removal of the rejection of Claim 1 as being unpatentably obvious of Schneier, at least by reason that Schneier also fails to teach, or suggest, (b) receiving, in said first device, from said second device a digital certificate encrypted using a first private key of said second device, and (c) receiving, in said first device, from said second device said first message encrypted using a second private key of said second device. Applicant again respectfully requests reconsideration and removal of all rejections of Claims 2 – 9, at least by virtue of these Claims' ultimate dependency upon a patentably distinct base Claim 1.

1.5. The Cited Portions of Schneier Do Not Teach or Suggest the Claimed Step (d) of Present Claim 1.

Claim 1 also recites, in part, "(d) authenticating said second device in response to said digital certificate and said first encrypted message." Thus, Claim 1 recites that the second device is authenticated responsively to the digital certificate received in step (b) and the encrypted first message received in step (c). Applicant submits Schneier fails to teach, or suggest, at least this limitation as well.

Applicant submits the present Office action admits so much, in that it argues, "[the] modified authentication scheme further discloses a final authentication step of A sending to B a third encrypted message comprising the data of B's identification garnered from B's digital certificate and encrypted using A's private key wherein B decrypts the third encrypted message using A's public key". *1/19/2005 Office action, par. 14, lines 16-19.* As the argued modification uses a third message to authenticate A, even *assuming arguendo* that this assertion is correct, it still fails to meet the recited limitation of step (d) of Claim 1 – which recites that the second device is authenticated responsively to the digital certificate received in step (b) and the encrypted first message received in step (c).

Accordingly, Applicant respectfully requests reconsideration and removal of the rejection of Claim 1 as being unpatentably obvious over Schneier, at least by

reason that Schneier also fails to teach, or suggest, authenticating said second device in response to said digital certificate and said first encrypted message. Applicant again respectfully requests reconsideration and removal of all rejections of Claims 2 – 9, at least by virtue of these Claims' ultimate dependency upon a patentably distinct base Claim 1.

1.6. The Cited Portions of Schneier Do Not Teach or Suggest the Claimed Step (e) of Present Claim 1.

Claim 1 also recites, in part, "(e) establishing a communication channel between said first and said second devices in response to the authentication of said second device." Applicant submits the cited portions of Schneier also fail to teach, or suggest, at least this limitation.

For non-limiting purposes of explanation, support for this limitation may be found on page 11, lines 20-24 of the specification, wherein it teaches, "[f]inally, STB 20 establishes a communication channel (see Figure 2, Step 190) between STB 20 and SP 40 wherein all future communication may be handled utilizing public-key cryptography and the public and private key pairs associated with SP 40 (i.e. KSPpub and KSPpri)."

The present Office action argues the Schneier steps of: node A receiving the principle message M encrypted with the symmetrical key K ($E_k(M)$) and the symmetrical key K encrypted by node A's public key ($E_A(K)$); decrypting the key message ($D_A(K)$), and then using the decrypted key K to retrieve message M ($D_k(M)$) "establishes a secure communications channel between the nodes." *1/19/2005 Office action, par. 12, lines 3-12.*

Applicant traverses this assertion. Completion of these steps merely provides node A access to message M. It does not establish a communication "channel", as the process would assumedly need to be repeated for other messages. Applicant submits the referenced portions of Schneier do not teach, or suggest, re-using symmetric key K for other communications. Indeed, the referenced portions of Schneier instead teach timestamps may be used to prohibit repeated use of

encrypted data (e.g., a digital signature). *See, e.g., Schneier, page 38, "Signing Documents and Timestamps".*

Further, Claim 1 requires that the communication channel be established responsively to the authentication of step (d). Applicant submits that to the extent the identified Schneier key and message exchange protocol establishes a communication channel, an assertion Applicant traverses, it is established in response to decryption of a symmetric key using a private key, and decryption of principle message (M) using the decrypted symmetric key, and not in response to an authentication, as is required by Claim 1. Accordingly, even *assuming arguendo* that such an assertion is true, the referenced teachings of Schneier still fails to satisfy the recited step (e) of Claim 1.

For at least the foregoing reasons, Applicant respectfully requests reconsideration and removal of the rejection of Claim 1 as being unpatentably obvious of Schneier, at least by reason that Schneier also fails to teach, or suggest, (e) establishing a communication channel between said first and said second devices in response to the authentication of said second device. Applicant again respectfully requests reconsideration and removal of all rejections of Claims 2 – 9, at least by virtue of these Claims' ultimate dependency upon a patentably distinct base Claim 1.

2. Claim 10 - A method for managing access to a device.

In similar fashion to that of Claim 1, independent method Claim 10 recites:

> A method for managing access to a device, said method comprising:
> (a) sending first identification data associated with a first device to a second device;
> (b) receiving, in said first device, from said second device a digital certificate encrypted using a first private key of said second device, said digital certificate having second identification data associated with said second device and a second public key of said second device;
> (c) encrypting said first identification data in said second device using a second private key associated with said second device to generate first encrypted identification data;

(d) receiving, in said first device, from said second device said first encrypted identification data;
(e) decrypting in said first device, using a first public key to obtain said second public key, said encrypted digital certificate received from said second device, said first public key being stored in said first device;
(f) decrypting said first encrypted identification data using said second public key to generate a first decrypted identification data;
(g) authenticating said second device by comparing said first decrypted identification data to said first identification data;
(h) sending to said second device second encrypted identification data, said second encrypted identification data being encrypted in said first device using said second public key of said second device; and
(i) establishing a communication channel between said first and said second devices.

Accordingly, Applicant respectfully submits present claim 10 is distinguishable over the cited art of record for at least the foregoing reasons. Wherefore, Applicant respectfully requests reconsideration and removal of the rejection of Claim 10 as well.

3. Rejection of claims 11-20 under 35 USC 103(a) as being unpatentable over Schneier in view of Arnold (U.S. Pat. 5,787,172) and/or Force (U.S. Pat. 5,533,123).

In similar fashion to that of Claim 1, independent Claim 11 recites:

A method for managing access between a service provider and a set-top box having a smart card coupled thereto, said set-top box performing the steps of:
(a) sending a first message to the smart card, said first message containing set-top box identification data;
(b) receiving from the smart card, in response to said first message, a first digital certificate encrypted using a first private key, said first digital certificate containing service provider identification data;
(c) authenticating the smart card in response to said first digital certificate;
(d) contacting the service provider in response to the authentication of the smart card and said service provider identification data and sending a second

message to the service provider, said second message containing set-top box identification data;

(e) receiving from the service provider, in response to said second message, a second digital certificate encrypted using a second private key of said service provider;

(f) receiving from the service provider said second message encrypted using a third private key;

(g) authenticating the service provider in response to said second digital certificate and said second encrypted message;

(h) providing confirmation of the authentication to the service provider; and

(i) establishing a communication channel with the service provider in response to the authenticated service provider.

Arnold is relied upon in the present Office action merely for its service provider, set-top box and smart card. Thus, Applicant respectfully submits it fails to remedy the significant shortcomings of Schneier discussed herein-above. Wherefore, Applicant respectfully requests reconsideration and removal of the rejection of Claim 11 as well.

Force is relied upon merely for purposes of its background teachings with regard to smartcards. Thus, Applicant respectfully submits Force fails to remedy the shortcomings of the teachings of Schneier and Arnold discussed above. Wherefore, Applicant respectfully requests reconsideration and removal of the rejection of Claim 12-20 as well, at least by virtue of these Claims' ultimate dependency upon a patentably distinct base Claim 11.

4. Conclusion

Entry of this response, for purposes of preserving the record for appeal, is respectfully requested.

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicant's attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully submitted,

Ahmet M. Eskicioglu, et al.

By: Paul P. Kiel
Attorney for Applicants
Registration No. 40,677

THOMSON Licensing Inc.
PO Box 5312
Princeton, NJ 08543-5312
Date: 3/10/05

CERTIFICATE OF MAILING

I hereby certify that this amendment is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to Mail Stop Amendment, Commissioner for Patents, Alexandria, Virginia 22313-1450 on:

3-11-05
Date

Lori Kleeman
~~Eliza Buchalczyk~~